

федеральное государственное бюджетное образовательное учреждение
высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Основная профессиональная образовательная программа
высшего образования программы бакалавриата по направлению подготовки

38.03.05 «Бизнес-информатика»

Направленность (профиль):
Бизнес-информатика

Квалификация:
Бакалавр

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Бизнес-информатика»

Степанов С.Ю. Степанов С.Ю.

Утверждаю
Председатель УМС И.И. Палкин И.И. Палкин

Рекомендована решением
Учебно-методического совета
19 июля 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 мая 2018 г., протокол № 5
Зав. кафедрой Бурлов В.Т.

Автор-разработчик:
Богданов П.Ю. Богданов П.Ю.

1. Цели освоения дисциплины

Цель дисциплины – изучение основных понятий, методов и средств обеспечения информационной безопасности личности, общества и государства.

Основные задачи дисциплины:

- формирование у студентов системы элементарных понятий, представлений и умений, связанных с обеспечением информационной безопасности, методологией систем защиты информации, общими принципами организации защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» для направления подготовки 38.03.05 «Бизнес-информатика» относится к дисциплинам базовой части блока обязательных дисциплин (модулей).

Для освоения данной дисциплины, обучающиеся должны освоить следующие дисциплины: «Правовая защита интеллектуальной собственности», «Информатика и программирование», «Управление данными предприятия», «Введение в профессиональную деятельность», «Основы бизнес-информатики», «Автоматизация деловых процессов», «Основы системного администрирования», «Операционные системы».

Параллельно с дисциплиной «Информационная безопасность» изучаются следующие дисциплины: «Основы Бизнес-информатики», «Автоматизация деловых процессов», «Бизнес-аналитика», «IT-бизнес», «Управление проектами», «IT-инфраструктура предприятия».

Дисциплина «Информационная безопасность» является базовой для освоения дисциплин: «Информационная безопасность в интернете», «Автоматизация деловых процессов», «Бизнес-аналитика», «IT-бизнес», «Управление проектами», «Бизнес-планирование», «Стратегическое планирование», «Разработка инновационных проектов».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих

компетенций:

Код компетенции	Компетенция
ОПК-1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-9	Организация взаимодействия с клиентами и партнерами в процессе решений задач управления информационной безопасностью ИТ-инфраструктуры предприятия.
ПК-21	Умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия.

В результате освоения компетенций в рамках дисциплины «Информационная безопасность» обучающийся должен:

Знать:

- сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
- основные криптографические протоколы;
- технологии, средства и методы обеспечения информационной безопасности телекоммуникационных систем.

Уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- применять криптографические средства и системы информационной безопасности.

Владеть:

- методами и средствами технической защиты информации;

- навыками рационального выбора средств и методов защиты информации объектов информатизации.

Основные признаки проявленности формируемых компетенций в результате освоения дисциплины «Информационная безопасность» сведены в таблицах 1, 2.

Таблица 1. Результаты обучения.

Код компетенции	Результаты обучения
ОПК-1	<p>Знать:</p> <ul style="list-style-type: none"> – основные понятия, свойства и виды информации; – методы и способы обработки данных; – основы функционирования Интернет. <p>Уметь:</p> <ul style="list-style-type: none"> – обрабатывать, сохранять, анализировать и изменять информацию в базовых программных продуктах профессиональной деятельности. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками работы с персональным компьютером.
ПК-9	<p>Знать:</p> <ul style="list-style-type: none"> – основные способы поиска информации с применением информационно-коммуникационных технологий. <p>Уметь:</p> <ul style="list-style-type: none"> – проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий; – систематизировать информацию; – проводить классификацию информационных систем для управления бизнесом; – определять рациональные информационные и ИКТ-решения для управления бизнесом. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками выбора и применения отечественных и зарубежных аналитических платформ, используемых для анализа инноваций в экономике, управлении и информационно - коммуникативных технологиях. – навыками пользования электронными ресурсами и прикладными программами для обработки информации; <p>технологиями аналитической обработки электронных массивов данных в целях исследования и анализа рынка информационных систем и информационно-коммуникативных технологий.</p>
ПК-21	<p>Знать:</p> <ul style="list-style-type: none"> – операционные среды, программное обеспечение и области их и эффективного применения. <p>Уметь:</p> <ul style="list-style-type: none"> – использовать основные информационно-коммуникационные технологии, операционные среды, программное обеспечение и

	<p>области их и эффективного применения.</p> <p>Владеть: информационно-коммуникационные технологиями, операционными средами, программным обеспечением.</p>
--	---

Таблица 2. Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания.

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании статистических методов	Способен выделить основные идеи статистических методов, работает со специальной литературой	Владеет основными навыками работы с источниками и критической литературой статистических методов	Способен дать собственную критическую оценку статистических методов
	не умеет	не выделяет основные идеи статистических методов	Способен показать основную идею в развитии статистических методов	Способен представить ключевую проблему статистических методов в ее связи с другими процессами	Может соотнести основные идеи статистических методов с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории статистических методов, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий статистических методов	Способен выделить характерный авторский подход статистических методов
базовый	не владеет	плохо ориентируется в терминологии и содержании статистических методов	Владеет приемами поиска и систематизации статистических методов, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций статистических методов	Способен сравнивать концепции статистических методов, аргументированно излагает материал
	не умеет	выделяет основные идеи статистических методов, но не видит проблем	Выделяет конкретную проблему статистических методов, однако излишне упрощает ее	Способен выделить и сравнить концепции статистических методов, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике статистических методов
	не знает	допускает много ошибок	Может изложить основные рабочие категории статистических методов	Знает основные отличия концепций статистических методов	Способен выделить специфику концепций в заданной проблемной области статистических методов
продвинутый	не владеет	ориентируется в терминологии и содержании статистических методов	В общих чертах понимает основную идею статистических методов, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем статистических методов, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем статистических методов
	не умеет	выделяет основные идеи статистических методов, но не видит их в развитии	Может понять практическое назначение основной идеи статистических методов, но затрудняется выявить ее основания	Выявляет основания заданной области статистических методов, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов статистических	Свободно ориентируется в заданной области анализа статистических методов. Понимает ее основания и умеет выделить практическое значение

				методов	статистических методов
	не знает	допускает ошибки при выделении рабочей области анализа статистических методов	Способен изложить основное содержание современных научных идей статистических методов	Знает основное содержание современных научных идей статистических методов, способен их сопоставить	Может дать критический анализ современным проблемам статистических методов

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины (модуля) для 2015, 2016 гг. составляет 4 зачетных единиц, 144 часа.

*Объем дисциплины (модуля) по видам учебных занятий
(в академических часах)
2015-2016 год набора*

Объём дисциплины	Всего часов		
	Очная форма обучения	Очно-заочная форма обучения	Заочная форма обучения
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	48	-	-
в том числе:			
лекции	16	-	-
практические занятия	34	-	-
лабораторная работа	-	-	-
Самостоятельная работа (СРС) – всего:	96	-	-
в том числе:			
курсовая работа	-	-	-
Вид промежуточной аттестации (зачет/экзамен)	экзамен	-	-

4.1. Структура дисциплины

Очная форма обучения

№ п/п	Раздел и тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.				Формы текущего контроля успеваемости	Занятия в активной и интерактивной форме, час.	Формируемые компетенции
			Лекции	Лаб. раб.	Прак. раб.	Сам.раб.			
1.	Введение.	7	4	-	8,5	24	Защита лабораторной работы. Ответ на вопрос по теме.	-	ОПК - 1; ПК-9; ПК-21
2.	Основные положения теории	7	4	-	8,5	24	Защита лабораторной работы. Ответ	-	ОПК - 1; ПК-9; ПК-21

	информационной безопасности.						на вопрос по теме.		
3.	Основы формальной теории защиты информации.	7	4	-	8,5	24	Защита лабораторной работы. Ответ на вопрос по теме.	-	ОПК - 1; ПК-9; ПК-21
4.	Стандарты в информационной безопасности.	7	4	-	8,5	24	Защита лабораторной работы. Ответ на вопрос по теме.	-	ОПК - 1; ПК-9; ПК-21
ИТОГО		16	-	34	96				

4.2. Содержание разделов дисциплины

Раздел и тема дисциплины	Содержание разделов дисциплины
Введение.	Область изучения. Введение. ИБ на территорию РФ. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.
Основные положения теории информационной безопасности.	Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система защиты информации. Общеметодологические принципы теории информационной безопасности.
Основы формальной теории защиты информации.	Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.
Стандарты в информационной безопасности.	Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тематика лабораторных занятий	Форма проведения	Формируемые компетенции
1	1	Введение.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
2	1	Основные положения теории информационной безопасности.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
3	1	Основы формальной теории защиты информации.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
4	1	Стандарты в информационной безопасности.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
5	2	Введение.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
6	2	Основные положения теории информационной безопасности.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
7	2	Основы формальной теории защиты информации.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
8	2	Стандарты в информационной безопасности.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21
9	2	Введение.	Изучение материалов урока, подготовка и выполнение заданий.	ОПК - 1; ПК-9; ПК-21

5. Учебно-методическое обеспечение самостоятельной работы студентов и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль включает оценку самостоятельной (внеаудиторной) и аудиторной работы (в том числе рубежный контроль).

Вид и формы контроля дисциплины: защита контрольной работы (для заочной формы обучения), защита лабораторной работы, ответ на вопрос по теме.

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студента в форме защиты выполненного отчета. Во время собеседования студент обязан проявить знания по достигнутой цели работы, теоретическому материалу, методам выполнения каждого этапа работы, содержанию основных разделов разработанного отчета с демонстрацией результатов на конкретных примерах. Студент обязан уметь правильно анализировать полученные результаты и объяснить физическую сущность полученных зависимостей и характеристик.

5.3. Промежуточный контроль: экзамен

Перечень вопросов к Экзамену:

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.

12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.
23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационная война как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.
30. Обеспечение безопасности объектов информационной сферы государства в информационной войне.
31. Компьютерная система как объект информационной безопасности.
32. Основные способы защиты информации.
33. Понятие и классификация средств защиты информации.
34. Характеристика средств защиты информации.

35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
37. Идентификация и аутентификация как сервисы безопасности.
38. Управление доступом и его виды.
39. Авторизация как сервис безопасности.
40. Протоколирование и аудит как сервисы безопасности.
41. Криптографические сервисы безопасности.
42. Экранирование как сервис безопасности.
43. Анализ защищенности как сервис безопасности.
44. Туннелирование как сервис безопасности.
45. Управление как сервис безопасности.
46. Назначение формальных моделей безопасности. Политика безопасности.
47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
49. Формальные модели целостности.
50. Понятие ролевого управления доступом.
51. Модели, стратегии и системы обеспечения информационной безопасности.
52. Критерии безопасности компьютерных систем «Оранжевая книга».
53. Общие критерии безопасности информационных технологий.
54. Критерии и классы защищенности СВТ и АС. Руководящие документы ФСТЭК России.
55. Стандарты по управлению информационной безопасностью ISO/IEC 27000.
56. Классификация и возможности технических разведок.
57. Компьютерная разведка.
58. Технические каналы утечки информации при эксплуатации автоматизированных систем.
59. Электромагнитное воздействие и эффекты его воздействия.
60. Защита автоматизированных систем и средств вычислительной техники

от внешнего

электромагнитного воздействия.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ананченко, И.В. Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие / И.В. Ананченко, П.И. Смирнов, Ю.М. Шапаренко. — СПб.: РГГМУ, 2016. — 24 с (Электронный ресурс) - Режим доступа: http://elib.rshu.ru/files_books/pdf/rid_934e2a15ca2e4a408df0517464e9941f.pdf
2. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. : С. А. Клейменова. - 2-е изд., стереотип. - Москва : Академия, 2007. - 330(1) с.
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2018. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-7088-3. — Режим доступа : www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83.

б) дополнительная литература:

1. Полякова Т.А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2017. — 325 с режим доступа: <https://biblio-online.ru/book/EF942E2F-1F06-44B2-B4E3-65F9A13F2735/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti>.
2. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1.
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAВ-68BB83EA616F.
4. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева.

— М. : Издательство Юрайт, 2018. — 349 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Режим доступа : www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2.

в) программное обеспечение и Интернет-ресурсы:

Программно-информационное обеспечение учебного процесса включает:

- Операционная система: Windows 7.
- Офисный пакет: Microsoft Office 2007.
- Gpg4win (GNU General Public License)
- GnuPG (GNU General Public License)
- Электронная библиотека ЭБС «Znanium» [Электронный ресурс]. Режим доступа: <http://znanium.com/>
- Электронная библиотека ЭБС «Юрайт» [Электронный ресурс]. Режим доступа: <https://biblio-online.ru/>
- Интерактивная онлайн-платформа по обучению [Электронный ресурс]. Режим доступа: <http://www.intuit.ru>
- Онлайн-версия КонсультантПлюс: Студент [Электронный ресурс]. Режим доступа: <http://student.consultants.ru>

7. Методические указания для обучающихся по освоению дисциплины

Вид учебных занятий	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать его преподавателю на консультации или на практическом занятии.
Лабораторные работы	На лабораторных работах студенты применяют теоретические знания на практике. Студенты изучают методические рекомендации к выполнению заданию. Преподаватель проводит консультации по изученному материалу. Обсуждаются задания и этапы работ. Выполняются лабораторные задания, изучаются примеры заданий. Кроме того, на лабораторных занятиях студенты представляют отчеты, подготовленные во время самостоятельной работы.
Внеаудиторная работа	представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает: <ul style="list-style-type: none"> – самостоятельное изучение разделов дисциплины; – выполнение дополнительных индивидуальных творческих заданий; – подготовку рефератов, сообщений и докладов.
Подготовка к зачету/экзамену	При подготовке к зачету/экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, вопросы для подготовки

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Тема 1 – Тема 4.	Чтение лекций с использованием слайд-презентаций, специализированных и офисных программ, информационных (справочных) систем, баз данных, организация взаимодействия с обучающимися посредством электронной почты.	Open Office, Блокнот

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины соответствует

действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов лекционных, практических, лабораторных занятий и самостоятельной работы бакалавров.

Учебный процесс обеспечен аудиториями, комплектом лицензионного программного обеспечения, библиотекой РГГМУ.

Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для проведения занятий практического типа – укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, ноутбук).

Учебная аудитория для курсового проектирования (выполнения курсовых работ) – укомплектована специализированной (учебной) мебелью.

Учебная аудитория для групповых и индивидуальных консультаций – укомплектована специализированной (учебной) мебелью, презентационной переносной техникой (проектор, ноутбук).

Учебная аудитория для текущего контроля и промежуточной аттестации – укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Лаборатория (компьютерный класс) – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет", обеспечено доступом в электронную информационно-образовательную среду организации, установлено необходимое специализированное программное обеспечение.